REMARKS

After the amendments contained herein, claims 1-12, 14-18, 20-23, and 25-29 remain pending in this application. The pending claims stand rejected. Claims 1, 26, and 29 are independent claims. The subject matter of dependent claim 19 has been incorporated herein into the independent claims, and claim 19 has been canceled without prejudice herein. The assignee traverses the rejections of the pending claims.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 2, 5-12, 14-23, and 25-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2003/0115448, application of Bouchard (Bouchard) in view of U.S. Publication No. 2002/0065042, application of Picoult, et al. (Picoult) and further in view of U.S. Publication No. 2004/0117456, application of Brooks (Brooks). These rejections are traversed.

As amended herein, claim 1 recites that the second attachment is automatically provided by the server to the mobile device when the secure message is opened in response to a user request. In rejecting this subject matter, the office action cited paragraph 46 and paragraph 48 (lines 1-22) of Brooks, stating that Brooks "discloses that the second attachment is automatically provided by the server to the mobile device when the secure message is opened in response to a user request." (Office action, p. 5.) The cited passages from Brooks, though, do not in any way disclose that a second attachment is automatically provided by a server to a mobile device when a secure message is opened in response to a user request. In fact, the cited passages do not teach anything at all about a user request to open a secure message. The cited passages from Brooks read as follows:

> [0046] For the embodiment, transmission software 112 provides separate transmission of email 108 and attachment 110 as follows. Email 108 and attachment identifier 114 are generated at computer 102 by transmission software 112 through attachment selection module 201. Graphical user interface 202, provided by attachment selection module 201, provides a user at computer 102 with an interface to enter information and parameters to be associated with attachment 110, such as a date and time when access to attachment 110 will expire, and an access password. As described in greater detail below, attachment identifier 114 includes information that uniquely identifies attachment identifier object 115 and attachment 110 to elements in network 100. When email 108 is sent from computer 102 to computer 104, attachment identifier 114 is sent with email 108 instead of attachment 110. Attachment identifier object 115 is also recorded into attachment identifier database 206, as described above, and attachment identifier 114 may then be used by computer 104 to retrieve attachment 110 from computer 102.
>
> [...]
>
> [0048] For the embodiment, server monitor module 208 establishes issuer communications path 122 between computer 102 and proxy server 106 through an Internet data stream via a TCP/IP port normally reserved for Internet data traffic, and thus provides a continuous connection between computer 102 and proxy server 106 to attempt to avoid interaction with data security interfaces that may be present between computer 102 and proxy server 106, such as firewalls or NAT systems. However, network security is not compromised through issuer communications path 122, since only attachment 110 can be accessed on computer 102 via attachment identifier 114 and such access is solely initiated and controlled by computer 102 and may also be password protected, as described below. The transmission of email 108 separately from attachment 110 provides a more secure delivery method for attachment 110 than prior art systems of email and file attachment transmission involving the transmission of email 108 together with attachment 110, since the transmission provided by the embodiment is encrypted, point to point, and strictly controlled via an access count, an expiry date, and/or an access password that is controlled by a user at computer 102, as described below. (Emphasis added.)

Brooks discloses in these paragraphs that a sender's computer 102 is used to establish parameters (via graphical user interface 202) with respect to an attachment that is to be sent separately from the email message to a recipient's computer 104. However, there is no teaching in these passages of a user request, let alone that opening a secure message in response to a user request acts as the "trigger" to automatically provide a second attachment to the mobile device as

required in claim 1. Because of the lack of teaching of this feature in any of the cited references of claim 1, claim 1 is allowable and should proceed to issuance.

The assignee disagrees with other positions in the office action as well. For example, claim 9 recites that a ***session key*** is received by the server from the mobile device for use by the server to decrypt the secure message. The office action relies on Bouchard in rejecting claim 9. Specifically, the office action cites paragraphs 62 and 63 of Bouchard, explaining that "the public key is available to both the server and mobile device." (Office action, p. 4.) The cited paragraphs of Bouchard read:

> If the satellite e-mail server 212 cannot receive messages from the master e-mail server 224, then the satellite e-mail server 212 discards any received message (STEP 708). If, however, the satellite e-mail server 212 determines that it can receive messages from the second organization's master e-mail server 224, the satellite e-mail server 212 decrypts the second encrypted e-mail 540 (STEP 712). Because the master e-mail server 224 encrypted the third e-mail 532 using the first organization's public key, the satellite e-mail server 224 decrypts the second encrypted e-mail 540 using its private key. Therefore, assuming that the private key of the satellite e-mail server 224 is secure and confidential (i.e., only the satellite e-mail server 224 "knows" the private key), the second encrypted e-mail 540 can only be decrypted by the satellite e-mail server 224. The server 212 then extracts the first encrypted e-mail 524 and transmits the e-mail 524 to the first organization's corporate e-mail server 216 over the main client-router communication channel 146 and the second client-router communication channel 143 (shown with arrow 258 in FIG. 2). The corporate e-mail server 216 performs its normal operations when receiving the first encrypted e-mail 524, such as scanning for viruses. The corporate e-mail server 216 then examines the recipient address of the first encrypted e-mail 524 and subsequently delivers the e-mail 524 to the user operating the desktop 220 over the main client-router communication channel 146 and the third client-router communication channel 144 (shown with arrow 262 in FIG. 2) (STEP 716).
>
> The desktop 220 receives the first encrypted e-mail 524. The desktop 220 then verifies the digital signature of the first encrypted e-mail 524. Because the master e-mail server 224 encrypted the second e-mail 508 with the second organization's private key, the desktop 220 needs the second organization's public key to decrypt the first encrypted e-mail 524. This key is public and typically available to anyone. Therefore, the desktop 220 obtains the public key of the second organization and uses

this public key to extract the second e-mail 508 from the first encrypted e-mail 524.

It is well-known in the art that a ***public key***, such as that discussed in the cited passage from Bouchard, does not disclose the use of a ***session key*** as recited in claim 9. Public keys are used as part of the set of encryption techniques referred to as asymmetric encryption, while session keys are used within the set of encryption techniques referred to as symmetric encryption. In symmetric encryption, the encryption key and the decryption key are identical. In asymmetric encryption, the encryption key, which is referred to as a "public key," is different than the decryption key, which is referred to as a "private key." As its name implies, a "public key" generally is freely available. Thus, the statement in the office action that "the public key is available to both the server and mobile device" is irrelevant to the claimed subject matter, which recites that a session key is received by the server. Unlike a public key, a session key cannot be freely shared, as any entity with access to a session key would be able to decrypt any message encrypted with the session key. Thus, for at least this reason, claim 9 is patentable over the cited references and should proceed to issuance.

As another example, claim 16 of the instant application recites "wherein the secure message is structured such that a secure layer has been added to the message and the second attachment, wherein the secure layer was generated during an encryption operation, wherein a ***decryption operation*** is performed in order to locate within the secure message the second attachment." In rejecting claim 16, the office action relies on paragraph 46 and paragraph 48 (lines 1-22) of Brooks, which passages were reproduced above. The passages from Brooks, though, do not teach that a decryption operation is performed at the server in order to locate within the secure message the second attachment. It is clear that claim 16 requires that the decryption operation is performed at the server since claim 1 recites "processing ***at the server*** the

secure message in order to locate within the secure message the second attachment." (Emphasis added.) Nothing in Brooks discloses performing a decryption operation (at the server) in order to locate within the secure message the second attachment as required by claim 16. For at least this reason, claim 16 is patentable over the cited references and should proceed to issuance.

In addition, Brooks logically cannot disclose the subject matter recited in claim 16 that the secure message is structured such that a secure layer has been added to the message and the second attachment. Brooks teaches throughout that an email (108) and attachment (110) are transmitted separately, not together. Thus, attachment 110 cannot be part of a secure message together with email 108, as that necessarily would involve email 108 and attachment 110 being transmitted together. Thus, for at least this additional reason, claim 16 is patentable over the cited references and should proceed to issuance.

Independent claims 26 and 29 recite subject matter analogous to the subject matter of claim 1. Thus, claims 26 and 29 are patentable over the cited references for at least the reasons set forth above with respect to claim 1. In addition, it is noted that the assignee has not provided arguments with respect to certain of the dependent claims in the instant application. This is done without prejudice to the assignee's right to present arguments regarding any of the dependent claims at any point in the future. Further, because each of the dependent claims in the instant application depends from a base claim that is itself allowable, the dependent claims are allowable for at least the reasons set forth with respect to the base claims.

CONCLUSION

For the foregoing reasons, assignee respectfully submits that the pending claims are allowable. Therefore, the examiner is respectfully requested to pass this case to issuance.

Respectfully submitted,

By: _____

Joseph M. Sauer
Reg. No. 47,919
JONES DAY
North Point
901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-3939